not entered
(not page for page)

TEXT AS AMENDED

CLAIMS

1. Method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \,.\, Q_i^v \equiv 1 \,.\, mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n;}$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv -\ g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2\ mod\ n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors $\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,\,j}}$ ($\mathbf{Q_{i,\,j} \equiv Q_i\ mod\ p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where **r** is a random value such that **0 < r < n,**

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1 , r_2 , \ldots r_f\}}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D,**

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{\ d1} \,.\, Q_2^{\ d2} . \ldots Q_m^{\ dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{\ d1} \,.\, Q_{i,2}^{\ d2} . \ldots Q_{i,m}^{\ dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}.**

2. Method according to claim 1, designed to prove the authenticity of an entity known as a demonstrator to an entity known as the controller, said demonstrator entity comprising the witness;

said demonstrator and controller entities executing the following steps:

• Step 1: act of commitment R

- at each call, the witness computes each commitment **R** by applying the process specified in claim 1,

- the demonstrator sends the controller all or part of each commitment **R**,

• **Step 2: act of challenge d**

- the controller, after having received all or part of each commitment **R**, produces challenges **d** whose number is equal to the number of commitments **R** and sends the challenges **d** to the demonstrator,

• **Step 3: act of response D**

- the witness computes the responses **D** from the challenges **d** by applying the process specified in claim 1,

• **Step 4: act of checking**

- the demonstrator sends each response **D** to the controller,

case where the demonstrator has transmitted a part of each commitment R

if the demonstrator has transmitted a part of each commitment **R**, the controller, having the **m** public values $G_1, G_2, \ldots, G_m$, computes a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . \bmod n$$

the controller ascertains that each reconstructed commitment **R'** reproduces all or part of each commitment **R** that has been transmitted to it.

case where the demonstrator has transmitted the totality of each commitment R

if the demonstrator has transmitted the totality of each commitment **R**, the controller, having the **m** public values $G_1, G_2, \ldots, G_m$, ascertains that each commitment **R** satisfies a relationship of the type

$$R \equiv G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v / G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . \bmod n$$

3. Method according to claim 1, designed to provide proof to an entity, known as the controller entity, of the integrity of a message **M** associated with an entity called a demonstrator entity, said demonstrator entity comprising the witness;

said demonstrator and controller entities executing the following steps:

- **Step 1: act of commitment R**

- at each call, the witness computes each commitment **R** by applying the process specified according to claim 1,

- **Step 2: act of challenge d**

- the demonstrator applies a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T,**

- the demonstrator sends the token **T** to the controller,

- the controller, after having received a token T, produces challenges **d** equal in number to the number of commitments **R** and sends the challenges **d** to the demonstrator,

- **Step 3: act of response D**

- the witness computes the responses **D** from the challenges **d** by applying the process specified according to claim 1,

- **Step 4: act of checking**

- the demonstrator sends each response **D** to the controller,

- the controller, having the **m** public values $\mathbf{G_1, G_2, ..., G_m}$, computes a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$\mathbf{R' \equiv G_1{}^{d1} . G_2{}^{d2} . ... G_m{}^{dm} . D^v \bmod n}$$

or a relationship of the type

$$\mathbf{R' \equiv D^v / G_1{}^{d1} . G_2{}^{d2} . ... G_m{}^{dm} . \bmod n}$$

- then the controller applies the hashing function **h** whose arguments are the message **M** and all or part of each reconstructed commitment **R'** to reconstruct the token **T'**,

- then the controller ascertains that the token **T'** is identical to the token **T** transmitted.

4. Method according to claim 1, designed to produce the digital signature of a message **M** by an entity known as the signing entity, said signing entity comprising the witness;

Signing operation

said signing entity executes a signing operation in order to obtain a signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

said signing entity executes the signing operation by implementing the following steps:

• **Step 1: act of commitment R**

- at each call, the witness computes each commitment **R** by applying the process specified according to claim 1,

• **Step 2: act of challenge d**

- the signing party applies a hashing function **h** whose arguments are the message **M** and each commitment **R** to obtain a binary train,

- from this binary train, the signing party extracts challenges **d** whose number is equal to the number of commitments **R**,

• **Step 3: act of response D**

- the witness computes the responses **D** from the challenges **d** by applying the process specified according to claim 1.

5. Method according to claim 4, designed to prove the authenticity of the message M by checking the signed message through an entity called a controller;

Checking operation

- said controller entity having the signed message executes a checking operation by proceeding as follows:

• **case where the controller has commitments R, challenges d, responses D**

if the controller has commitments **R**, challenges **d**, responses **D**,

• • the controller ascertains that the commitments **R**, the challenges **d** and the responses **D** satisfy relationships of the type

$$\mathbf{R \equiv G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . D^v \bmod n}$$

or relationships of the type

$$\mathbf{R \equiv D^v/G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . \bmod n}$$

• • the controller ascertains that the message **M**, the challenges **d** and the commitments **R** satisfy the hashing function:

$$\mathbf{d = h\ (message, R)}$$

• case where the controller has challenges d and responses D

if the controller has challenges **d** and responses **D**,

• • the controller reconstructs, on the basis of each challenge **d** and each response **D**, commitments **R'** satisfying relationships of the type

$$\mathbf{R' \equiv G_1{}^{d1} . G_2{}^{d2} . \ldots G_{\mathit{m}}{}^{dm} . D^v \bmod n}$$

or relationships of the type:

$$\mathbf{R' \equiv D^v/G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . \bmod n}$$

• • the controller ascertains that the message **M** and the challenges **d** satisfy the hashing function:

$$\mathbf{d = h\ (message, R')}$$

• case where the controller has commitments R and responses D

if the controller has commitments **R** and responses **D**,

• • the controller applies the hashing function and reconstructs **d'**

$$\mathbf{d' = h\ (message, R)}$$

• • the controller device ascertains that the commitments **R,** the challenges **d'** and the responses **D** satisfy relationships of the type

$$\mathbf{R \equiv G_1{}^{d'1} . G_2{}^{d'2} . \ldots G_m{}^{d'm} . D^v \bmod n}$$

or relationships of the type:

$$\mathbf{R \equiv D^v/G_1{}^{d'1} . G_2{}^{d'2} . \ldots G_m{}^{d'm} . \bmod n}$$

6. A system designed to prove, to a controller server,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of:

- **m** pairs of private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1, or parameters derived from these values,

- a public modulus **n** constituted by the product of said **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2, said modulus and said values being linked by relations of the type

$$\mathbf{G_i . Q_i^v \equiv 1 . mod\ n}\text{ or }\mathbf{G_i \equiv Q_i^v\ mod\ n} .$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of the base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \dots p_f}$, the base number $\mathbf{g_i}$ being such that the following conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n}\quad\text{and}\quad\mathbf{x^2 \equiv - g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2\ mod\ n}$$

can be resolved in x in the ring of the integers modulo **n;**

said system comprises a witness device, contained especially in a nomad object which, for example, takes the form of a microprocessor-based bank card,

the witness device comprises

- a memory zone containing the **f** prime factors $\mathbf{p_i}$ and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or **f.m** components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i\ mod\ p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v;**

said witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments **R** of the witness device, to compute commitments **R** in the ring of integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v\ mod\ n}$$

where **r** is a random value produced by the random value production means, r being such that $0 < r < n$,

• or by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$, then by applying the Chinese remainder method;

said witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges **d** of the witness device, to receive one or more challenges **d**; each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges;

- computation means, hereinafter called means for the computation of the responses **D** of the witness device for the computation, on the basis of each challenge **d, of** a response **D**,

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1^{\;d1} \,.\, Q_2^{\;d2} \ldots Q_m^{\;dm} \bmod n$$

• or by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}^{\;d1} \,.\, Q_{i,2}^{\;d2} \ldots Q_{i,m}^{\;dm} \bmod p_i$$

and then by applying the Chinese remainder method.

- transmission means to transmit one or more commitments **R** and one or more responses **D;**

there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}.**

7. A system according to claim 6, designed to prove the authenticity of an entity called a demonstrator and an entity called a controller,

said system being such that it comprises:

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified according to claim 1,

the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device through the connection means;

• **Step 2: act of challenge d**

the controller device comprises challenge production means for the production, after receiving all or part of each commitment **R**, of the challenges **d** equal in number to the number of commitments **R,**

the controller device also has transmission means, hereinafter known as the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

• **Step 3: act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 1,

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller,

the controller device also comprises:

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment R.

if the transmission means of the demonstrator have transmitted a part of each commitment **R**, the computation means of the controller device, having **m** public values **G_1, G_2, ..., G_m**, compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1{}^{d1} . G_2{}^{d2} . ... G_m{}^{dm} . D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v/G_1{}^{d1} . G_2{}^{d2} . ... G_m{}^{dm} . \bmod n$$

the comparison means of the controller device compare each reconstructed commitment **R'** with all or part of each commitment **R** received,

case where the demonstrator has transmitted the totality of each commitment R

if the transmission means of the demonstrator have transmitted the totality of each commitment **R**, the computation means and the comparison means of the controller device, having **m** public values **G_1, G_2, ..., G_m**, ascertain that each commitment **R** satisfies a relationship of the type

$$R \equiv G_1{}^{d1} . G_2{}^{d2} . ... G_m{}^{dm} . D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v/G_1{}^{d1} . G_2{}^{d2} . ... G_m{}^{dm} . \bmod n$$

8. System according to claim 6, designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator,

said system being such that it comprises

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified in claim 1

the witness device has transmission means, hereinafter called transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• **Step 2: act of challenge d**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T,**

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T** through the connection means to the controller device,

the controller device also has challenge production means for the production, after having received the token **T**, of the challenges **d** in a number equal to the number of commitments **R**, the controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means;

- **Step 3: act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 1,

- **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller,

the controller device also comprises computation means, hereinafter called the computation means of the controller device, having **m** public values $\mathbf{G_1, G_2, ..., G_m}$, to firstly compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$\mathbf{R' \equiv G_1{}^{d1} . G_2{}^{d2} . ... G_m{}^{dm} . D^v \bmod n}$$

or a relationship of the type

$$\mathbf{R' \equiv D^v / G_1{}^{d1} . G_2{}^{d2} . ... G_m{}^{dm} . \bmod n}$$

then, secondly, compute a token **T'** by applying the hashing function **h** having as arguments the message **M** and all or part of each reconstructed commitment **R'**,

the controller device also has comparison means, hereinafter known as the comparison means of the controller device, to compare the computed token **T'** with the received token **T**.

9. System according to claim 6, designed to produce the digital signature of a message **M**, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message **M**,

- the challenges **d** and/or the commitments **R**,
- the responses **D**;

Signing operation

said system being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said system enabling the execution of the following steps:

- **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified according to claim 1, the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

- **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**,

- **Step 3: act of response D**

the means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means,

the means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 1,

the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses **D** to the signing device through the interconnection means.

10. System according to claim 9, designed to prove the authenticity of the message **M** by checking the signed message by means of an entity called the controller;

Checking operation

the system being such that it comprises a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the signing device;

the signing device associated with the signing entity comprises transmission means, hereinafter known as the transmission means of the signing device, for the transmission, to the controller device, of the signed message through the connection means, in such a way that the controller device has a signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

the controller device comprises:

- computation means hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device.

• case where the controller device has commitments R, challenges d, responses D

if the controller has commitments **R**, challenges **d**, responses **D**,

• • the computation and comparison means of the controller device ascertain that the commitments **R**, the challenges **d** and the responses **D** satisfy relationships of the type

$$\mathbf{R \equiv G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . D^v \bmod n}$$

or relationships of the type:

$$\mathbf{R \equiv D^v/G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . \bmod n}$$

• • the computation and comparison means of the controller device ascertain that the message **M**, the challenges **d** and the commitments **R** satisfy the hashing function:

d = h (message, R)

• case where the controller device has challenges d and responses D

if the controller device has challenges **d** and responses **D**,

• • the computation means of the controller, on the basis of each challenge **d** and each response **D**, compute commitments **R'** satisfying relationships of the type

$$\mathbf{R' \equiv G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . D^v \bmod n}$$

or relationships of the type:

$$\mathbf{R' \equiv D^v/G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . \bmod n}$$

• • the computation and comparison means of the controller device ascertain that the message **M** and the challenges **d** satisfy the hashing function:

d = h (message, R')

• case where the controller device has commitments R and responses D

if the controller device has commitments **R** and responses **D**,

• • the computation means of the controller device apply the hashing function and compute **d'** such that

d' = h (message, R)

• • the computation and comparison means of the controller device ascertain that the commitments **R**, the challenges **d'** and the responses **D** satisfy relationships of the type

$$\mathbf{R \equiv G_1{}^{d'1} . G_2{}^{d'2} . \ldots G_m{}^{d'm} . D^v \bmod n}$$

or relationships of the type:

$$\mathbf{R \equiv D^v/G_1{}^{d'1} . G_2{}^{d'2} . \ldots G_m{}^{d'm} . \bmod n}$$

11. A terminal device associated with an entity, taking the form especially of a nomad object, for example the form of a microprocessor in a microprocessor-based bank card, designed to prove to a controller server:

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity;

by means of :

- **m** pairs of private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1, or parameters derived from these values,

- a public modulus **n** constituted by the product of said **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$ (**f** being greater than or equal to 2),

said modulus and said values being related by relations of the type

$$\mathbf{G_i \,.\, Q_i^v \equiv 1 \,.\, mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n}\ .$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1.

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of the base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$, the base number $\mathbf{g_i}$ being such that:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv - g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2\ mod\ n}$$

can be resolved in x in the ring of the integers modulo **n.**

said terminal device comprises a witness device comprising,

- a memory zone containing the **f** prime factors $\mathbf{p_i}$ and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or **f.m** components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i\ mod\ p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v**.

said witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments **R** of the witness device, to compute commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^{v} \bmod n}$$

where **r** is a random value produced by the random value production means, r being such that $\mathbf{0 < r < n}$,

• or by performing operations of the type:

$$\mathbf{R_i \equiv r_i^{v} \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1 , r_2 , \ldots r_f\}}$ produced by the random value production means, then by applying the Chinese remainder method;

said witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges **d** of the witness device, to receive one or more challenges **d**; each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges;

- computation means, hereinafter called means for the computation of the responses **D** of the witness device, for the computation, on the basis of each challenge **d,** of a response **D,**

• either by performing operations of the type:

$$\mathbf{D \equiv r . Q_1^{\ d1} . Q_2^{\ d2}. \ldots Q_m^{\ dm} \bmod n}$$

• or by performing operations of the type:

$$\mathbf{D_i \equiv r_i . Q_{i,1}^{\ d1} . Q_{i,2}^{\ d2}. \ldots Q_{i,m}^{\ dm} \bmod p_i}$$

and then by applying the Chinese remainder method,

- transmission means to transmit one or more commitments **R** and one or more responses **D**;

there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}.**

12. A terminal device according to claim 11, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller.

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device also comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device enabling the execution of the following steps:

- **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified according to claim 1,

the witness device has transmission means, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device, through the connection means;

- **Steps 2 and 3: act of challenge d, act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 1,

- **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller that carries out the check.

13. Terminal device according to claim 11, designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator,

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device being used to execute the following steps:

- **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified according to claim 1; the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

- **Steps 2 and 3: act of challenge d, act of response D**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**,

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T,** through the connection means, to the controller device,

said controller, after having received the token **T**, produces challenges **d** equal in number to the number of commitments **R**, the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 1,

- **Step 4: act of checking**

the transmission means of the demonstrator send each response **D** to the controller device which performs the check.

14. Terminal device according to claim 11, designed to produce the digital signature of a message **M**, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

said terminal device being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking especially the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

Signing operation

said terminal device being used to execute the following steps:

- **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified according to claim 1, the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the signing device through the interconnection means,

- **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**,

- **Step 3: act of response D**

the means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means, the means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 1,

the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses **D** to the signing device, through the interconnection means.

15. Controller device especially taking the form of a terminal or remote server associated with a controller entity, designed to check:

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity

by means of:

- **m** pairs of public values $\mathbf{G_1}, \mathbf{G_2}, \ldots \mathbf{G_m}$, **m** being greater than or equal to 1,
- a public modulus **n** constituted by the product of said **f** prime factors $\mathbf{p_1}, \mathbf{p_2}, \ldots \mathbf{p_f}$, **f** being greater than or equal to 2, unknown to the controller device and to the associated controller entity,

said modulus and said values being related by relations of the type

$$G_i . Q_i^v \equiv 1 . \bmod n \text{ or } G_i \equiv Q_i^v \bmod n .$$

where Q_i designates a private value, unknown to the controller device, associated with the public value G_i.

v designating a public exponent such that

$$v = 2^k$$

where k is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the f prime factors $p_1, p_2, \ldots p_f$, the base number g_i being such that the following conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv - g_i \bmod n$$

can be resolved in x in the ring of integers modulo n

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo n.

16. Controller device according to claim 15, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller;

said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a demonstrator device associated with the demonstrator entity;

sid controller device being used to execute the following steps:

- **Steps 1 and 2: act of commitment R, act of challenge d**

said controller device also has means for the reception of all or part of the commitments **R** coming from the demonstrator device through the connection means, the controller device has challenge production means for the production, after receiving all or part of each commitment **R**, of the challenges **d** in a number equal to the number of commitments **R**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges.

the controller device also has transmission means, hereinafter called transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means;

• **Steps 3 and 4: act of response D, act of checking**

said controller device also comprises:

- means for the reception of the responses D coming from the demonstrator device, through the connection means,

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment R.

if the reception means of the demonstrator have received a part of each commitment **R**, the computation means of the controller device, having **m** public values $\mathbf{G_1}$, $\mathbf{G_2}$, ..., $\mathbf{G_m}$, compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$\mathbf{R' \equiv G_1{}^{d1} . G_2{}^{d2} . .... G_m{}^{dm} . D^v \bmod n}$$

or a relationship of the type

$$\mathbf{R' \equiv D^v / G_1{}^{d1} . G_2{}^{d2} . .... G_m{}^{dm} . \bmod n}$$

the comparison means of the controller device compare each reconstructed commitment **R'** with all or part of each commitment **R** received,